(12)特許協力条約に基づいて公開された国際出願

549293

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年12 月9 日 (09.12.2004)

PCT

(10) 国際公開番号
WO 2004/107339 A1

(51) 国際特許分類[7]: G11B 20/10, 20/12, G09C 1/00

(21) 国際出願番号: PCT/JP2004/006900

(22) 国際出願日: 2004 年5 月14 日 (14.05.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-150906 2003 年5 月28 日 (28.05.2003) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 海老原 宗毅 (EBIHARA, Munetake) [JP/JP]. 勝股 充 (KATSUMATA, Mitsuru) [JP/JP]. 久野 浩 (KUNO, Hiroshi) [JP/JP]. 林 隆道 (HAYASHI, Takamichi) [JP/JP].

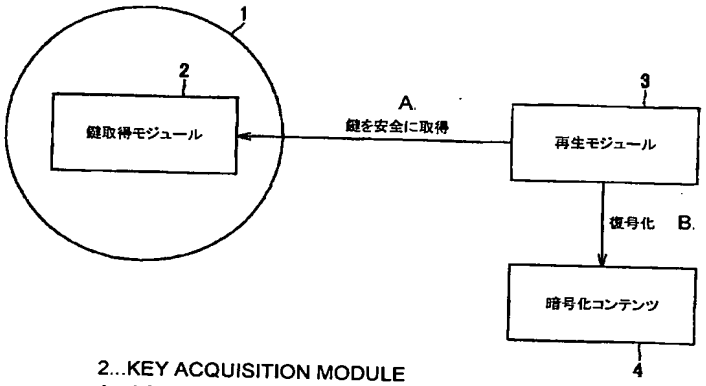
(74) 代理人: 中村 友之 (NAKAMURA, Tomoyuki); 〒1050001 東京都港区虎ノ門１丁目２番３号虎ノ門第一ビル９階 三好内外国特許事務所内 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE,

[続葉有]

(54) Title: INFORMATION RECORDING MEDIUM, INFORMATION PROCESSING DEVICE AND METHOD

(54) 発明の名称: 情報記録媒体、並びに情報処理装置及び方法



2...KEY ACQUISITION MODULE
A...ACQUIRE KEY SAFELY
3...REPRODUCTION MODULE
B...DECRYPTION
4...ENCRYPTED CONTENT

(57) Abstract: It is possible to prevent unauthorized copying of recorded information and flexibly operate a content. Furthermore, it is possible to facilitate improvement of the copy prevention technique. A key acquisition module (2) is recorded on an information recording medium (1) dedicated to reading and having the copy prevention technique. A reproduction module (3) safely acquires a medium key inherent to the key acquisition module (2) from the key acquisition module (2), generates a content key from the medium key, decrypts the encrypted content (4) by using the content key, and reproduces it. Here, the key acquisition module (2) should be resident on the information recording medium (1) while the reproduction module (3) and the encrypted content (4) need not be on the information recording medium (1) but may be outside the information recording medium (1).

(57) 要約: 記録された情報の不法コピーを防止すると共にコンテンツの柔軟な運用を可能とし、さらにコピー防止技術の改良等も容易とする。鍵取得モジュール（２）は、コピー防止技術が施された読み取り専用の情報記録媒体（１）に記録されている。再生モジュール（３）は、この鍵取得モジュール（２）から該鍵取得モジュール（２）に固有のメディア鍵を安全に取得し、このメディア鍵からコンテンツ鍵を生成し、このコンテンツ

[続葉有]

WO 2004/107339 A1

SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

鍵を用いて暗号化コンテンツ（４）を復号化して再生する。ここで、鍵取得モジュール（２）は情報記録媒体（１）上に存在する必要があるが、再生モジュール（３）及び暗号化コンテンツ（４）は情報記録媒体（１）上に存在する必要はなく、情報記録媒体（１）の外部に存在していても構わない。

明細書

情報記録媒体、並びに情報処理装置及び方法

技術分野

本発明は、コンテンツの不正利用を防止すると共にコンテンツの柔軟な運用を可能とし、さらにコピー防止技術の改良等も容易とする情報記録媒体、並びにそのような情報記録媒体を用いてコンテンツを再生する情報処理装置及びその方法に関する。

背景技術

近年において、光ディスク等の情報記録媒体の大容量化と普及により、記録されている情報の著作権を保護するために、不法なコピーの防止が重要とされてきている。すなわち、オーディオデータやビデオデータの場合には、コピー或いはダビングにより劣化のない複製物を容易に生成でき、またコンピュータデータの場合には、元のデータと同一のデータが容易にコピーできるため、既に不法コピーによる著作権の侵害等の弊害が生じてきているのが実情である。

このようなことから、上記不法コピーの防止を目的として、コピーコントロールＣＤ（Copy Control Compact Disk；ＣＣＣＤ）と称されるレッドブック規格外の音楽ＣＤが開発・販売されるに至っている。このＣＣＣＤのセカンドセッションエリアに記録されているオーディオデータについては、ＣＣＣＤ上に記録されている専用の再生モジュールを用いてパーソナルコンピュータでの再生が可能であるものの、パーソナルコンピュータ内部へ取り込み（リッピング）ができず、コピーが防止されるようになされている。

また、同様に不法コピーの防止を目的として、ＳｅｃｕＲＯＭ（登録商標）と称されるＣＤ－ＲＯＭ（Compact Disk - Read Only Memory）も開発・販売されている。このＳｅｃｕＲＯＭでは、サブコード（Ｑサブチャンネル）に隠蔽されたコピー防止キーを抽出し、該コピー防止キーを用いて、少なくともその一部が暗号化されたアプリケーションを復号化することで、該アプリケーションを実行することができるものの、不法コピーされている場合には、アプリケーションを暗号化したコピー防止キーとは異なるものが抽出され、該アプリケーションを実行することができない（特開平１１－２５０５１２号公報）。

しかしながら、このような従来のＣＣＣＤやＳｅｃｕＲＯＭ（登録商標）においては、媒体とそれに記録された音楽情報（コンテンツ）とが不可分であるため、コンテンツを媒体から切り離して運用することができず、運用の柔軟性がないという問題があった。また、媒体のコピー防止技術を改良しようとした場合、その媒体に記録されたコンテンツを再生するパーソナルコンピュータ等にインストールしなければならないソフトウェアが複雑化してしまう虞があった。

本発明は、このような従来の実情に鑑みて提案されたものであり、コンテンツの不正利用を防止すると共にコンテンツの柔軟な運用を可能とし、さらにコピー防止技術の改良等も容易とする情報記録媒体、並びにそのような情報記録媒体を用いてコンテンツを再生する情報処理装置及びその方法を提供することを目的とする。

発明の開示

上述した目的を達成するために、本発明に係る情報記録媒体は、第１の実行ファイルが複製不可に記録された情報記録媒体であり、この第１の実行ファイルは、第２の実行ファイルとの間で認証処理を行う認証手

段と、該第１の実行ファイルに固有の固有鍵情報を取得する鍵取得手段と、上記固有鍵情報を上記第２の実行ファイルに送信する送信手段とを有し、情報記録媒体が情報処理装置に挿入されたときに実行されるものである。

このような情報記録媒体に記録された第１の実行ファイルは、情報記録媒体が情報処理装置に挿入されたときに実行され、第２の実行ファイルとの間で相互に認証処理を行い、第１のファイルに固有の固有鍵情報を第２のファイルに送信する。

また、上述した目的を達成するために、本発明に係る情報処理装置は、第１の実行ファイルが複製不可に記録された情報記録媒体が挿入される情報処理装置であって暗号化されたコンテンツを再生する第２の実行ファイルを有し、この第２の実行ファイルは、上記第１の実行ファイルとの間で認証処理を行う認証手段と、上記第１の実行ファイルから取得した固有鍵情報に基づいて暗号鍵情報を生成する鍵生成手段と、上記暗号鍵情報を用いて上記暗号化されたコンテンツを復号化する復号化手段と、復号化した上記コンテンツを再生する再生手段とを有し、上記情報記録媒体が挿入されたときに実行されるものである。

このような情報処理装置が有する第２の実行ファイルは、第１の実行ファイルが複製不可に記録された情報記録媒体が挿入されたときに実行され、第１の実行ファイルとの間で相互に認証処理を行い、第１のファイルから取得した固有鍵情報に基づいて暗号鍵情報を生成し、この暗号鍵情報を用いて暗号化されたコンテンツを復号化して再生する。

また、上述した目的を達成するために、本発明に係る情報処理方法は、第１の実行ファイルが複製不可に記録された情報記録媒体が挿入される情報処理装置の情報処理方法であり、上記第１の実行ファイルとの間で認証処理を行う認証工程と、上記第１の実行ファイルから取得した固有

鍵情報に基づいて暗号鍵情報を生成する鍵生成工程と、上記暗号鍵情報を用いて暗号化されたコンテンツを復号化する復号化工程と、復号化した上記コンテンツを再生する再生工程とを有するものである。

このような情報処理方法では、情報記録媒体に記録された第１の実行ファイルとの間で相互に認証処理を行い、第１のファイルから取得した固有鍵情報に基づいて暗号鍵情報を生成し、この暗号鍵情報を用いて暗号化されたコンテンツを復号化して再生する。

図面の簡単な説明

第１図は、本実施の形態の概念構成を説明する図である。

第２図は、鍵取得モジュールがメディア鍵を取得して再生モジュールに転送するまでの処理の一例を説明するフローチャートである。

第３図は、鍵取得モジュールがメディア鍵を取得して再生モジュールに転送するまでの処理の他の例を説明するフローチャートである。

第４図は、再生モジュールが鍵取得モジュールから鍵を取得し、暗号化コンテンツを復号化して再生するまでの処理を説明するフローチャートである。

第５図は、再生モジュールが鍵取得モジュールから鍵を取得し、暗号化コンテンツを情報処理装置にインポートするまでの処理を説明するフローチャートである。

第６図は、本実施の形態における情報処理装置の構成例を示す図である。

発明を実施するための最良の形態

以下、本発明を適用した具体的な実施の形態について、図面を参照しながら詳細に説明する。

先ず、本実施の形態の概念構成について、第１図を用いて説明する。第１図において、鍵取得モジュール２（第１の実行ファイル）は、コピー防止技術が施された読み取り専用の情報記録媒体１に記録されている。このコピー防止技術としては、例えばＳｅｃｕＲＯＭ（登録商標）に用いられている技術や、いわゆるダミーファイル法の技術が挙げられるが、これらに限定されず種々の技術を用いることができる。再生モジュール３（第２の実行ファイル）は、この鍵取得モジュール２から該鍵取得モジュール２に固有のメディア鍵（固有鍵情報）を安全に取得し、このメディア鍵からコンテンツ鍵（暗号鍵情報）を生成し、このコンテンツ鍵を用いて暗号化コンテンツ４を復号化して再生する。

このように、本実施の形態では、コンテンツが暗号化された状態で提供され、その暗号化コンテンツ４の復号化に用いられるメディア鍵がコピー防止技術の施された情報記録媒体１に記録されているため、暗号化コンテンツ４がコピーされた場合であっても正規の情報記録媒体１がなければメディア鍵を取得できず、コンテンツを利用することができない。

ここで、本実施の形態における鍵取得モジュール２は情報記録媒体１上に存在する必要があるが、再生モジュール３及び暗号化コンテンツ４は情報記録媒体１上に存在する必要はなく、情報記録媒体１の外部に存在していても構わない。つまり、再生モジュール３及び暗号化コンテンツ４の配置形態としては、

１）情報記録媒体１上に再生モジュール３及び暗号化コンテンツ４が存在する場合、

２）情報記録媒体１の外部に再生モジュール３及び暗号化コンテンツ４が存在する場合、

３）情報記録媒体１上に再生モジュール３が存在し、情報記録媒体１の外部に暗号化コンテンツ４が存在する場合、

４）情報記録媒体１の外部に再生モジュール３が存在し、情報記録媒体１上に暗号化コンテンツ４が存在する場合、の４通りが考えられる。

以下では、再生モジュール３及び暗号化コンテンツ４が情報記録媒体１の挿入される情報処理装置に存在する場合（上記２の場合）について、主として説明する。この再生モジュール３及び暗号化コンテンツ４は、予めネットワークを介して情報処理装置にダウンロードしたものであっても構わない。なお、以下では、情報記録媒体１は読み出し専用の光ディスクであるものとする。

先ず、情報記録媒体１のコピー防止技術としてＳｅｃｕＲＯＭ（登録商標）の技術が用いられている場合に、鍵取得モジュール２がメディア鍵を取得し、このメディア鍵を再生モジュール３に転送するまでの処理を第２図のフローチャートに示す。

このＳｅｃｕＲＯＭ（登録商標）の技術とは、簡単には、予め情報記録媒体１上の所定のアドレス及び個数のサブコード（Ｑサブチャンネル）を変更しておき、アプリケーションを暗号化するコピー防止キーとしてその変更パターンを用いるものである。アプリケーションを実行する際には、上記所定のアドレス及び個数のＱサブチャンネルを検索し、その変更パターンからコピー防止キーを抽出する。ここで、情報記録媒体１をコピーした場合、変更が施されていた正規でないＱサブチャンネルは正規のＱサブチャンネルとしてコピーされる。この結果、元々アプリケーションを暗号化していたものとは異なるコピー防止キーが抽出されることとなり、アプリケーションを復号化して実行することができない。なお、この第２図に示すコピー防止技術については、例えば特開平１１－２５０５１２号公報に記載されている。

具体的には、始めに第２図のステップＳ１において、鍵取得モジュール２は、暗号化されていない例えば前半部分のプログラムにより、情報

記録媒体１上の所定のアドレス及び個数のサブコード（Ｑサブチャンネル）をスキャンし、ステップＳ２において、そのＱサブチャンネルが正規であるか否かを検索する。次にステップＳ３において、鍵取得モジュール２は、正規でないＱサブチャンネルの数に応じてコピー防止キーを抽出する。そしてステップＳ４では、抽出したコピー防止キーを用いて鍵取得モジュール２の後半部分の暗号を復号化できるか否かが判別される。ステップＳ４において復号化できる場合（Yes）にはステップＳ５に進み、復号化できない場合（No）には処理を終了する。ステップＳ５において、鍵取得モジュール２は、再生モジュール３との間で認証処理を行い、ステップＳ６では、認証の適否が判別される。ステップＳ６において相互に認証しない場合（No）には処理を終了し、相互に認証する場合（Yes）にはステップＳ７においてメディア鍵を再生モジュール３に転送する。

一方、情報記録媒体１のコピー防止技術としていわゆるダミーファイル法の技術が用いられている場合に、鍵取得モジュール２がメディア鍵を取得し、このメディア鍵を再生モジュール３に転送するまでの処理を第３図のフローチャートに示す。

このダミーファイル法の技術とは、簡単には、情報記録媒体１のサイズよりも大きいダミーファイルが実際に情報記録媒体１に記録されているかのように予めディレクトリレコードを変更しておき、アプリケーションを実行する際にそのダミーファイルのサイズを検査するものである。この情報記録媒体１をコピーする場合には、例えばディレクトリレコードのダミーファイルサイズを実際のダミーファイルのサイズに一致させる必要があるが、アプリケーションの実行前にそのダミーファイルのサイズが元のサイズ（情報記録媒体１のサイズよりも大きいサイズ）と一致するか否かが検査され、一致しない場合にはアプリケーションの実行

が許可されない。なお、この第３図に示すコピー防止技術については、例えば特開２００１－２２９０１９号公報に記載されている。

具体的には、始めに第３図のステップＳ１０において、鍵取得モジュール２はダミーファイルを開き、ステップＳ１１において、そのダミーファイルのファイルサイズを検査する。次にステップＳ１２において、鍵取得モジュール２は、そのファイルサイズが元のファイルサイズと一致するか否かを判別し、一致しない場合（No）には処理を終了する。一方、一致する場合（Yes）にはステップＳ１３に進む。ステップＳ１３において、鍵取得モジュール２は、再生モジュール３との間で認証処理を行い、ステップＳ１４では、認証の適否が判別される。ステップＳ１４において相互に認証しない場合（No）には処理を終了し、相互に認証する場合（Yes）にはステップＳ１５においてメディア鍵を再生モジュール３に転送する。

次に、再生モジュール３が鍵取得モジュール２から鍵を取得し、暗号化コンテンツ４を復号化して再生するまでの処理を第４図のフローチャートに示す。ステップＳ２０において、再生モジュール３は、鍵取得モジュール２がロード可能であるか否かを判別し、ロード可能でない場合（No）には処理を終了し、ロード可能である場合（Yes）にはステップＳ２１に進む。次にステップＳ２１において、再生モジュール３は、鍵取得モジュール２との間で認証処理を行い、ステップＳ２２では、認証の適否が判別される。ステップＳ２２において相互に認証しない場合（No）には処理を終了し、相互に認証する場合（Yes）にはステップＳ２３において鍵取得モジュール２からメディア鍵を取得する。

続いてステップＳ２４において、再生モジュール３は、取得したメディア鍵からコンテンツ鍵を生成し、ステップＳ２５において、このコンテンツ鍵を用いて暗号化コンテンツ４の復号化を行う。なお、この暗号

化コンテンツ４は、情報記録媒体１が挿入される情報処理装置内に存在するものであっても、ネットワークを介してダウンロードしたものであっても構わない。そしてステップＳ２６において、コンテンツを再生可能であるか否かが判別され、再生不可である場合（No）には処理を終了し、再生可能である場合（Yes）にはステップＳ２７でコンテンツを再生する。

なお、上述した第４図では、暗号化コンテンツ４を再生する場合について説明したが、情報記録媒体１に暗号化コンテンツ４が記録されている場合には、この暗号化コンテンツ４を情報処理装置にインポートすることも可能である。このような場合において、再生モジュール３が鍵取得モジュール２から鍵を取得し、暗号化コンテンツ４を情報処理装置にインポートするまでの処理を第５図のフローチャートに示す。なお、ステップＳ３４においてコンテンツ鍵を生成するまでの処理は上述した第４図と同様であるため説明を省略する。

ステップＳ３５において、再生モジュール３は、生成したコンテンツ鍵を用いて、例えば暗号化コンテンツ４に付属する権利情報及び暗号署名のうち、暗号署名を復号化して権利情報の検証を行う。なお、この権利情報及び暗号署名は、情報記録媒体１上に存在するものであっても、ネットワークを介してダウンロードしたものであっても構わない。そしてステップＳ３６において、インポートが許可されるか否かが判別され、インポートが許可されない場合（No）には処理を終了し、インポートが許可される場合（Yes）にはステップＳ３７で暗号化コンテンツ４をインポートする。

以下、上述した情報処理装置の具体的な構成例について第６図を用いて説明する。第６図に示すように、情報処理装置１０は、該情報処理装置１０の各部を統括して制御するＣＰＵ（Central Processing

Unit）１１と、不揮発性のメモリであるＲＯＭ（Read Only Memory）１２と、揮発性のメモリであるＲＡＭ（Random Access Memory）１３と、通信処理を行う通信部１４と、図示しないハードディスクに対して各種データの書き込み及び／又は読み出しを行うＨＤＤ（Hard Disk Drive）１５と、音声を出力する出力部１６と、情報記録媒体１に対して各種データの書き込み及び／又は読み出しを行うインターフェース（Ｉ／Ｆ）部１７とがバス１８を介して相互に接続されてなる。

ＣＰＵ１１は、例えばＲＯＭ１２に記録されているプログラムに従って、プログラムを実行するための制御を行う。ＲＡＭ１３には、ＣＰＵ１１が各種処理を実行する上で必要なプログラムやデータが必要に応じて一時的に格納される。

通信部１４は、例えばモデムやターミナルアダプタ等により構成され、電話回線を介してインターネットに接続される。

ＨＤＤ１５は、図示しないハードディスクからデータの読み出しを行うほか、例えば通信部１４を介して入力したデータの書き込みを行う。

オーディオ出力部１６は、例えば通信部１４を介して入力したオーディオデータや、インターフェース部１７を介して情報記録媒体１から入力したオーディオデータに対して、必要に応じて変換を施して出力する。

インターフェース部１７は、ＣＰＵ１１の制御のもとに、情報記録媒体１に対してデータを入出力するタイミングを調整し、データの形式を変換する。

このような情報処理装置１０において、再生モジュール３は、例えばＨＤＤ１５に記録されており、情報記録媒体１に記録された鍵取得モジュール２との間で上述した処理を行い、メディア鍵を取得する。そして、再生モジュール３は、このメディア鍵からコンテンツ鍵を生成し、このコンテンツ鍵を用いて、例えば通信部１４を介して入力してＨＤＤ１５

に記録された暗号化コンテンツ４を復号化する。復号化されたコンテンツは、ＣＰＵ１１の制御のもと、オーディオ出力部１６から出力される。

以上説明したように、本実施の形態における情報記録媒体１及び情報処理装置１０によれば、コンテンツが暗号化された状態で提供され、その暗号化コンテンツ４の復号化に用いられるメディア鍵がコピー防止技術の施された情報記録媒体１に記録されているため、暗号化コンテンツ４がコピーされた場合であっても正規の情報記録媒体１がなければメディア鍵を取得できず、コンテンツを利用することができない。これにより、コンテンツの保護が図られる。

特に、暗号化コンテンツ４は情報記録媒体１上に存在する必要はなく、情報記録媒体１の外部に存在していても構わないため、情報記録媒体１の購入者のみが復号化できるような暗号化コンテンツ４をネットワークを介して配布するなど、コンテンツの柔軟な運用が可能となる。

また、再生モジュール３は、鍵取得モジュール２からメディア鍵を取得し、そのメディア鍵からコンテンツ鍵を生成して暗号化されたコンテンツを復号化するのみであり、情報記録媒体１にどのようなコピー防止技術が施されているかには依存しないため、コピー防止技術を改良した場合に、情報処理装置１０に新たなソフトウェア等をインストールする必要がない。

なお、本発明は上述した実施の形態のみに限定されるものではなく、本発明の要旨を逸脱しない範囲において種々の変更が可能であることは勿論である。

例えば、上述の実施の形態では、コンテンツがオーディオデータであるものとして説明したが、これに限定されるものではなく、ビデオデータなど他種のデータであっても構わない。

以上詳細に説明したように、本発明に係る情報記録媒体、並びに情報処理装置及びその方法によれば、情報記録媒体に複製不可に記録された第１の実行ファイルと第２の実行ファイルとの間で相互に認証処理を行った後、第１の実行ファイルから第２の実行ファイルに固有鍵情報を送信し、第２の実行ファイルでは、この固有鍵情報に基づいて暗号鍵情報を生成し、この暗号鍵情報を用いて暗号化されたコンテンツを復号化して再生することにより、コンテンツの不正利用が防止されると共に、コンテンツの柔軟な運用が可能となり、さらにコピー防止技術の改良も容易となる。

請求の範囲

1．　第１の実行ファイルが複製不可に記録された情報記録媒体であって、

上記第１の実行ファイルは、第２の実行ファイルとの間で認証処理を行う認証手段と、該第１の実行ファイルに固有の固有鍵情報を取得する鍵取得手段と、上記固有鍵情報を上記第２の実行ファイルに送信する送信手段とを有し、上記情報記録媒体が情報処理装置に挿入されたときに実行される

ことを特徴とする情報記録媒体。

2．　上記固有鍵情報は、コンテンツを暗号化する暗号鍵情報を暗号化するために用いられることを特徴とする請求の範囲第１項記載の情報記録媒体。

3．　上記第２の実行ファイル又は上記コンテンツは、上記情報記録媒体、上記情報処理装置又は他の情報処理装置に記録されていることを特徴とする請求の範囲第２項記載の情報記録媒体。

4．　上記コンテンツは、上記情報記録媒体に記録されており、

上記固有鍵情報は、上記コンテンツに付属する署名情報を暗号化する暗号鍵情報を暗号化するために用いられ、

上記送信手段は、上記署名情報に基づいて上記コンテンツを上記第２の実行ファイルに送信する

ことを特徴とする請求の範囲第３項記載の情報記録媒体。

5．　第１の実行ファイルが複製不可に記録された情報記録媒体が挿入される情報処理装置であって、

暗号化されたコンテンツを再生する第２の実行ファイルを有し、

上記第２の実行ファイルは、上記第１の実行ファイルとの間で認証処理を行う認証手段と、上記第１の実行ファイルから取得した固有鍵情報に基づいて暗号鍵情報を生成する鍵生成手段と、上記暗号鍵情報を用いて上記暗号化されたコンテンツを復号化する復号化手段と、復号化した上記コンテンツを再生する再生手段とを有し、上記情報記録媒体が挿入されたときに実行される

ことを特徴とする情報処理装置。

６．　上記暗号化されたコンテンツは、上記情報記録媒体、上記情報処理装置又は他の情報処理装置に記録されていることを特徴とする請求の範囲第５項記載の情報処理装置。

７．　上記暗号化されたコンテンツは、上記情報記録媒体に記録されており、

上記固有鍵情報は、上記暗号化されたコンテンツに付属する署名情報を暗号化する暗号鍵情報を暗号化するために用いられ、

上記第２の実行ファイルは、上記署名情報に基づいて上記第１の実行ファイルから上記暗号化されたコンテンツを受信する受信手段を有する

ことを特徴とする請求の範囲第６項記載の情報処理装置。

８．　第１の実行ファイルが複製不可に記録された情報記録媒体が挿入される情報処理装置の情報処理方法であって、

上記第１の実行ファイルとの間で認証処理を行う認証工程と、

上記第１の実行ファイルから取得した固有鍵情報に基づいて暗号鍵情報を生成する鍵生成工程と、

上記暗号鍵情報を用いて暗号化されたコンテンツを復号化する復号化工程と、

復号化した上記コンテンツを再生する再生工程と

を有することを特徴とする情報処理方法。

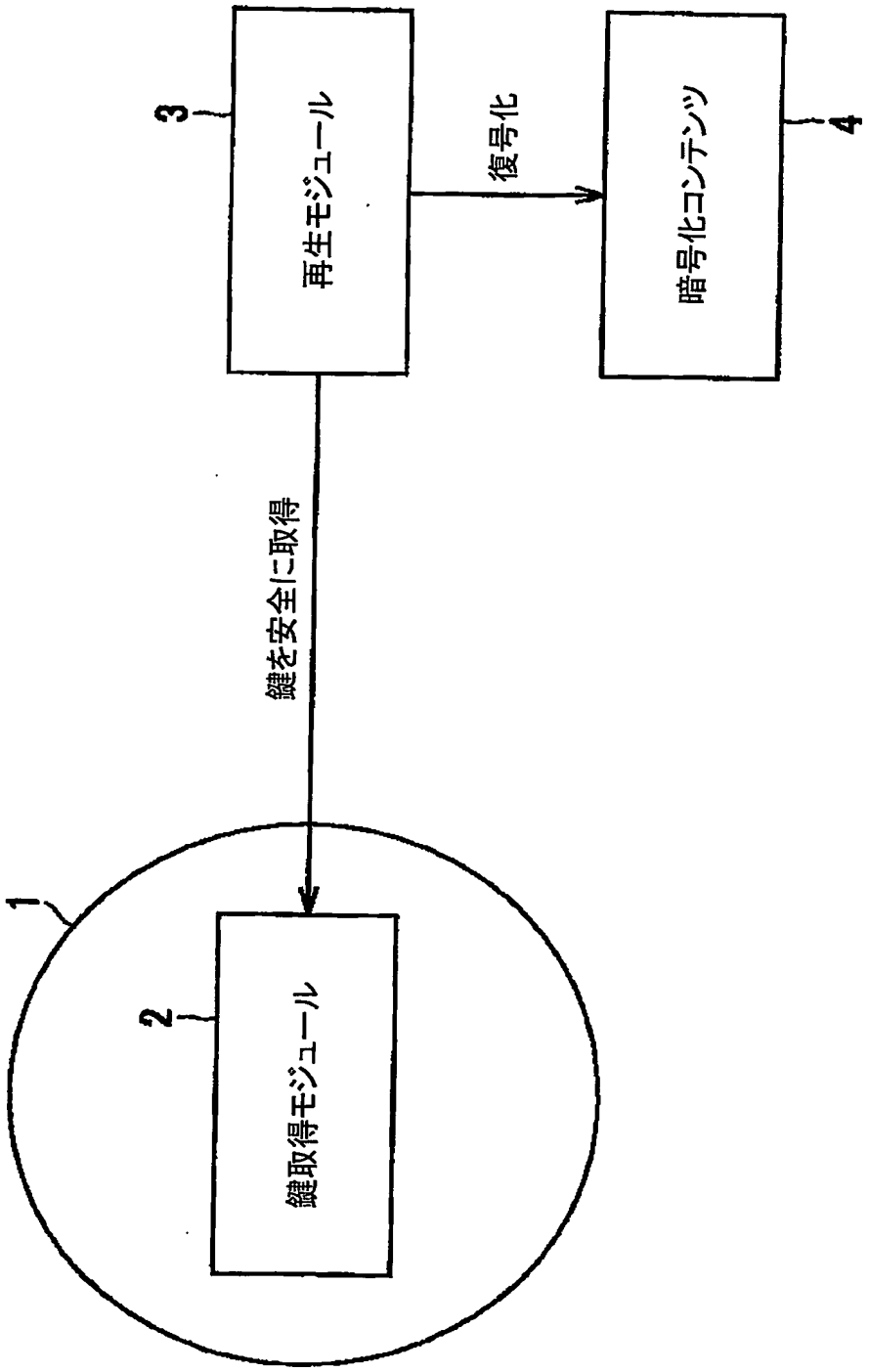


Fig.1

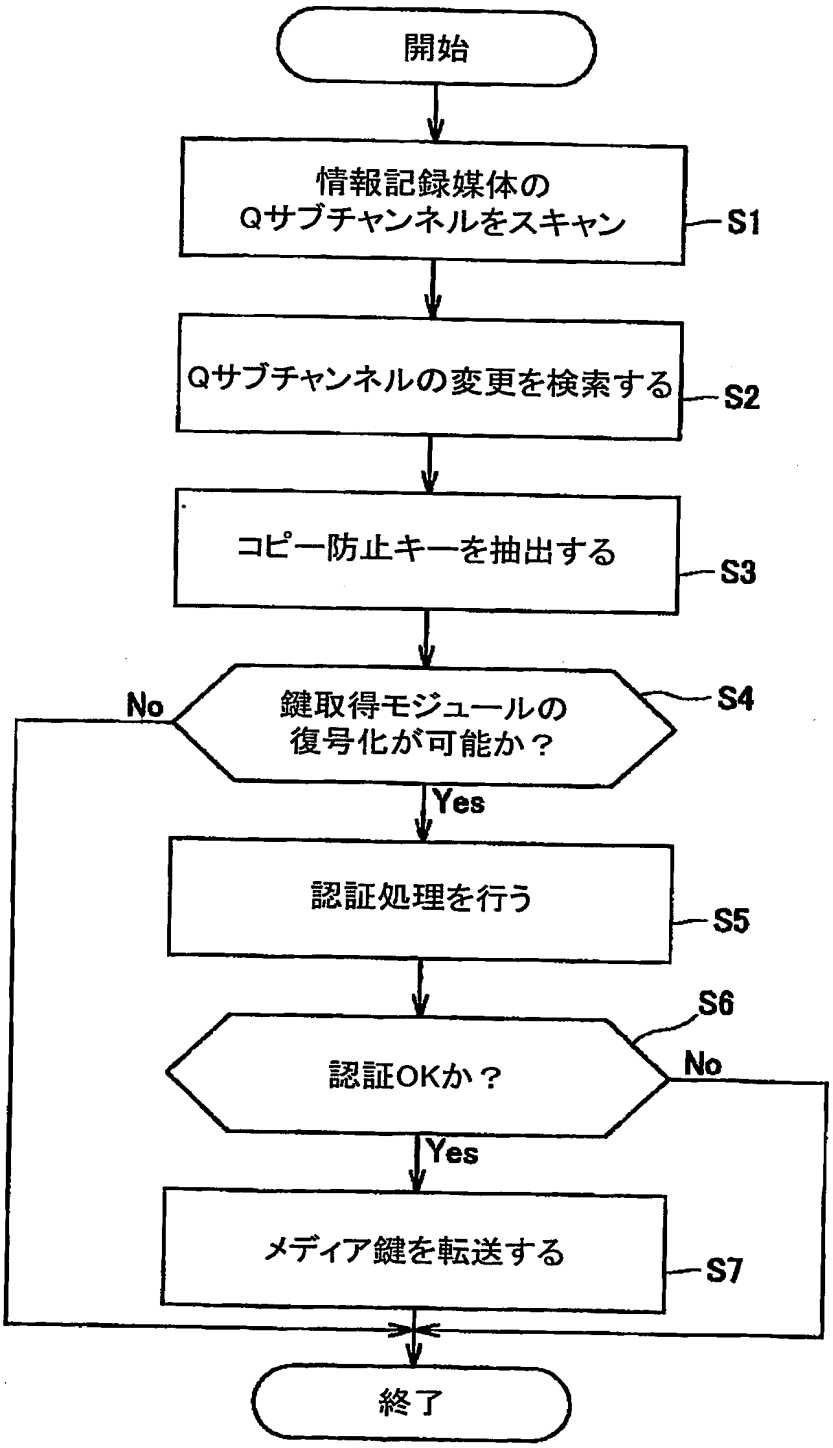

開始
情報記録媒体の
Qサブチャンネルをスキャン
S1
Qサブチャンネルの変更を検索する
S2
コピー防止キーを抽出する
S3
No
鍵取得モジュールの
復号化が可能か？
S4
Yes
認証処理を行う
S5
S6
認証OKか？
No
Yes
メディア鍵を転送する
S7
終了

Fig.2

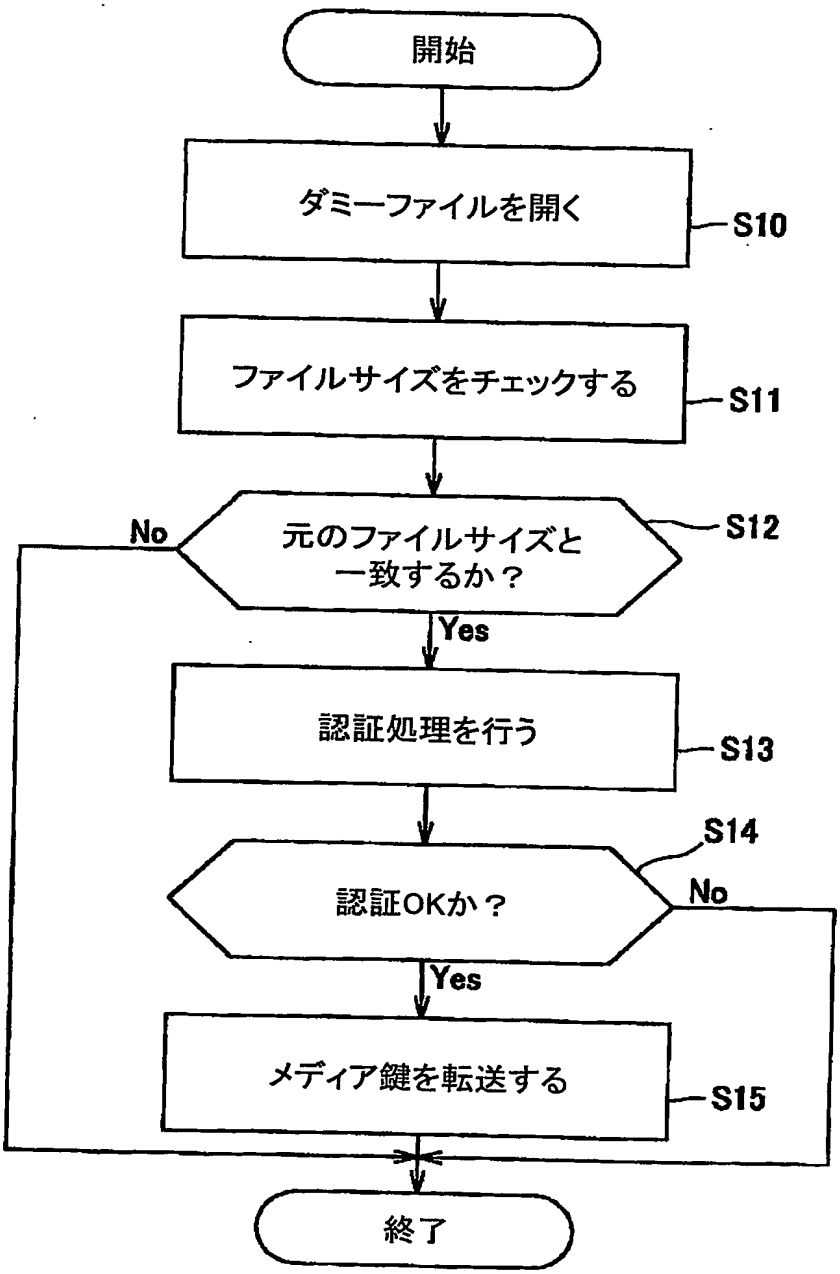

開始
ダミーファイルを開く
S10
ファイルサイズをチェックする
S11
No
元のファイルサイズと
一致するか？
S12
Yes
認証処理を行う
S13
S14
認証OKか？
No
Yes
メディア鍵を転送する
S15
終了

Fig.3

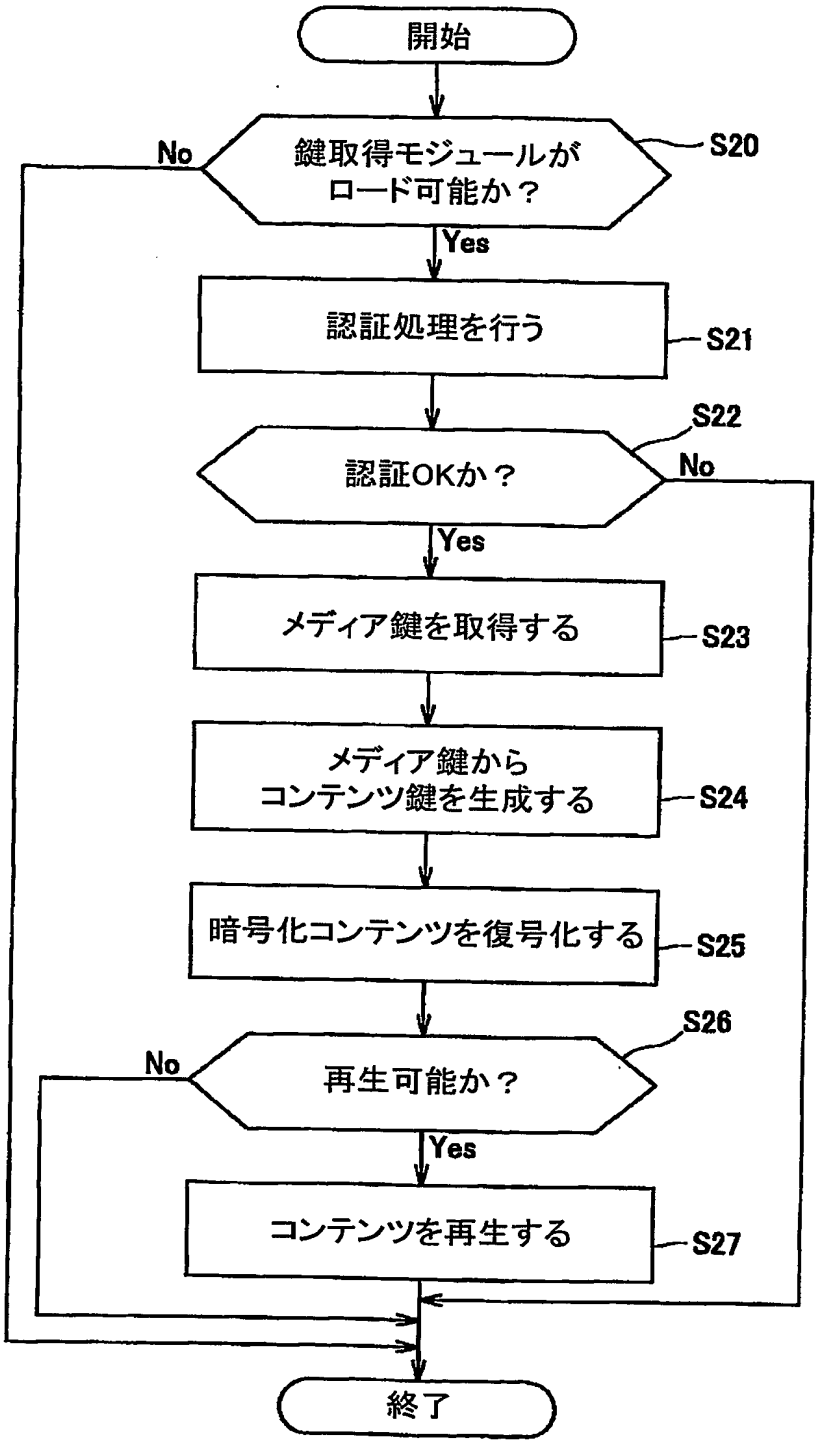

開始
鍵取得モジュールがロード可能か？
S20
No
Yes
認証処理を行う
S21
S22
認証OKか？
No
Yes
メディア鍵を取得する
S23
メディア鍵からコンテンツ鍵を生成する
S24
暗号化コンテンツを復号化する
S25
S26
No
再生可能か？
Yes
コンテンツを再生する
S27
終了

Fig.4

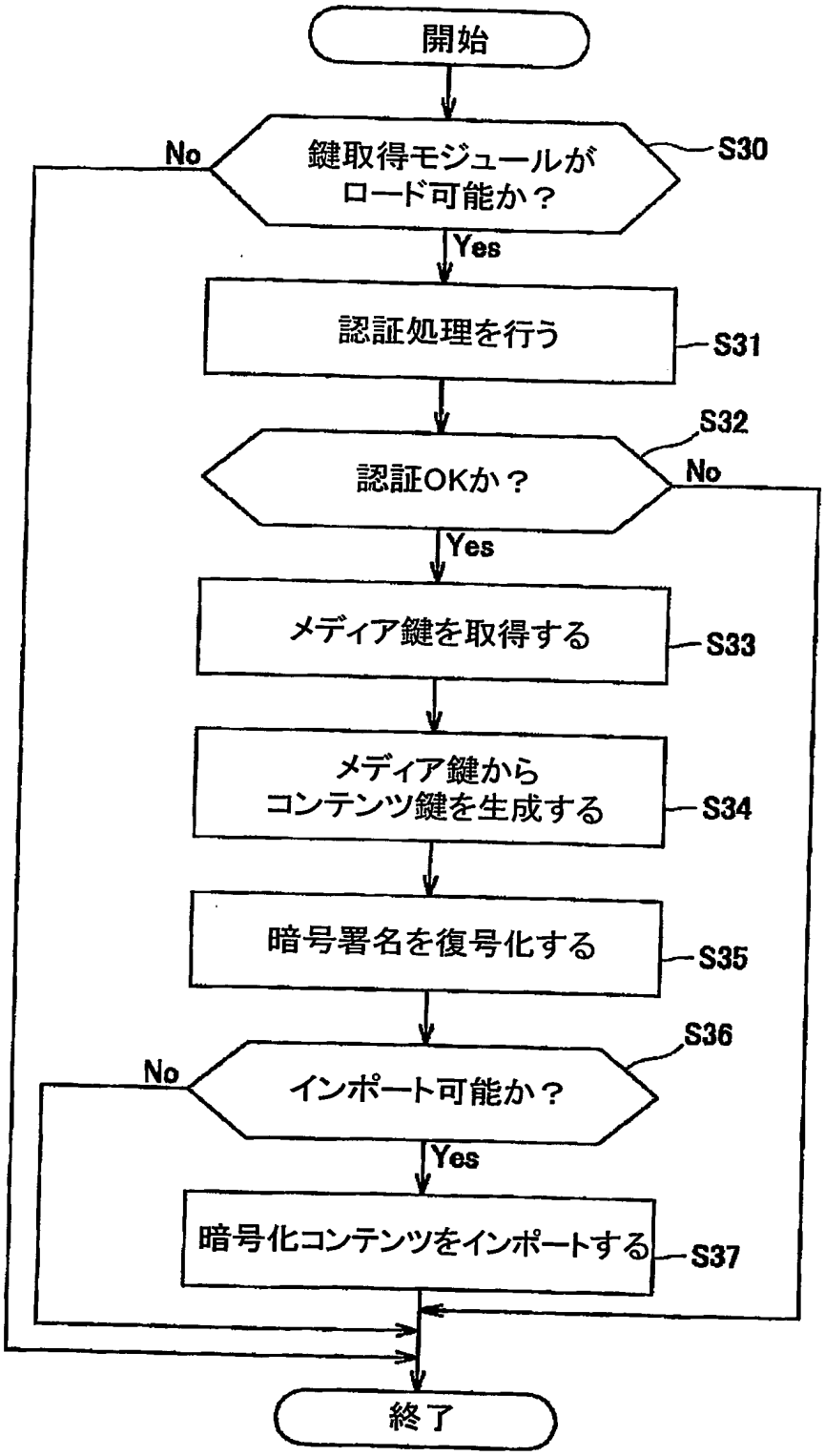

開始
鍵取得モジュールがロード可能か？
No
S30
Yes
認証処理を行う
S31
S32
認証OKか？
No
Yes
メディア鍵を取得する
S33
メディア鍵からコンテンツ鍵を生成する
S34
暗号署名を復号化する
S35
S36
No
インポート可能か？
Yes
暗号化コンテンツをインポートする
S37
終了

Fig.5

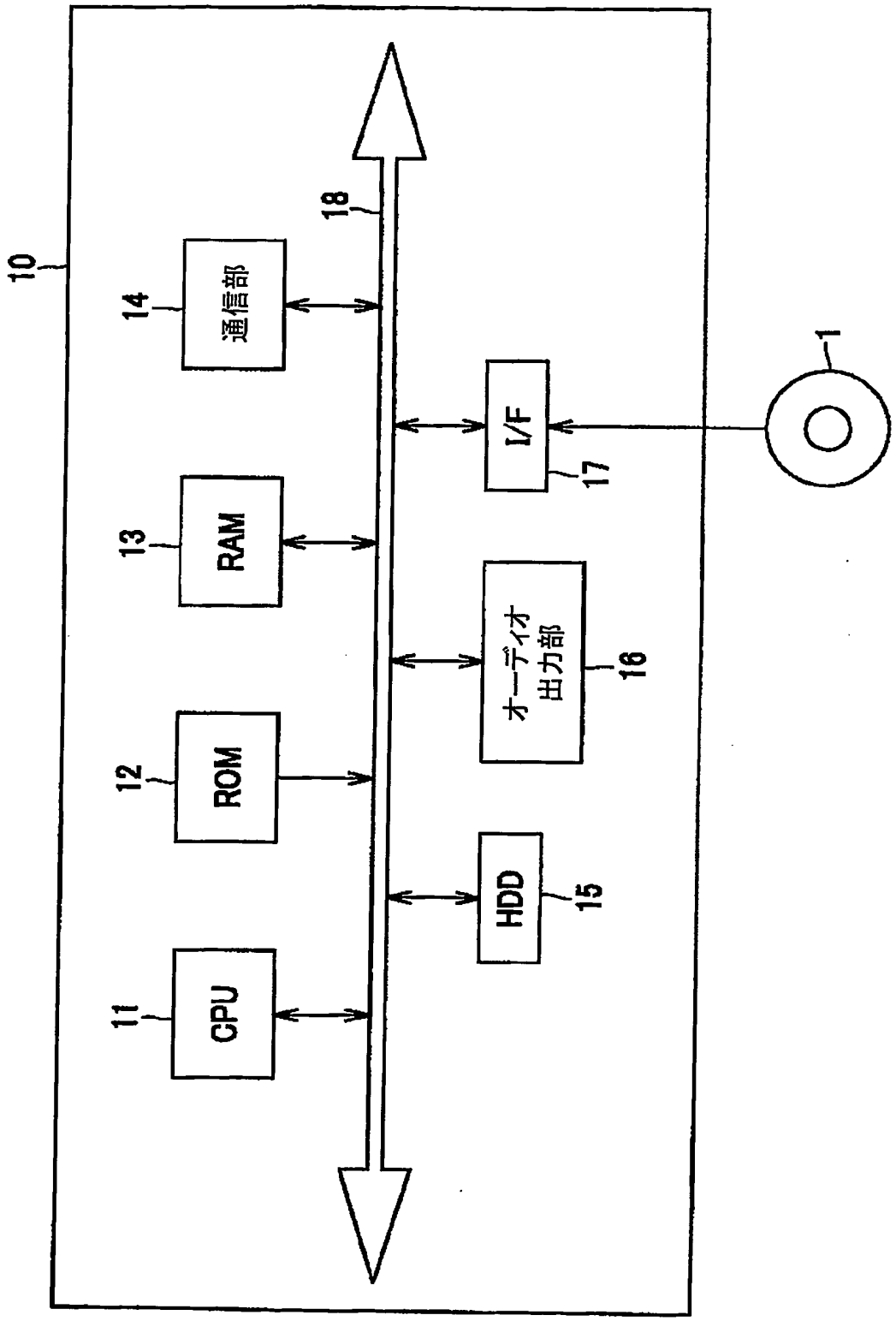


Fig.6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/006900

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G11B20/10, 20/12, G09C1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G11B20/10-20/16, G06F12/14, G09C1/00, H04L9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2002-100116 A (Sony Corp.), 05 April, 2002 (05.04.02), Column 22, line 35 to column 23, line 32; column 25, line 47 to column 26, line 5; column 29, line 3 to column 30, line 43; column 31, lines 32 to 37; Figs. 1, 2, 5 to 8 & EP 1302944 A1 & EP 1302945 A1 & US 2002/157012 A1 & US 2002/184537 A1	1-8
Y	JP 2002-63075 A (Sony Corp.), 28 February, 2002 (28.02.02), Column 3, lines 26 to 32; column 5, lines 5 to 18; column 6, lines 1 to 7; Fig. 1 (Family: none)	1-8

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 August, 2004 (13.08.04)	31 August, 2004 (31.08.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/006900

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-14441 A (Matsushita Electric Industrial Co., Ltd.), 19 January, 2001 (19.01.01), Column 11, lines 19 to 47; column 14, line 34 to column 15, line 38; Figs. 5, 6, 9 & EP 1050887 A1 & EP 1304702 A1	4,7
Y	JP 10-13403 A (NEC Corp.), 16 January, 1998 (16.01.98), Column 7, lines 21 to 41; column 9, line 23 to column 11, line 21; Figs. 1 to 5 (Family: none)	4,7
Y	JP 10-123950 A (Fuji Xerox Co., Ltd.), 15 May, 1998 (15.05.98), Column 14, line 32 to column 17, line 12; column 23, line 1 to column 24, line 21; Figs. 1, 3 to 5, 18, 19 & EP 837383 A1 & US 6161183 A	4,7
A	JP 11-250512 A (Sony DADC Austria AG.), 17 September, 1999 (17.09.99), Full text; Figs. 1 to 9 & EP 899733 A1 & US 6535858 B	1-8
A	JP 2001-229019 A (Toshiba EMI Ltd.), 24 August, 2001 (24.08.01), Full text; Figs. 1 to 9 (Family: none)	1-8

国際調査報告

国際出願番号　PCT／JP2004／006900

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ G11B20／10, 20／12, G09C1／00

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ G11B20／10－20／16, G06F12／14, G09C1／00,
H04L9／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2004年
日本国登録実用新案公報	1994－2004年
日本国実用新案登録公報	1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP　2002－100116　A（ソニー株式会社） 2002．04．05，第22欄第35行～第23欄第32行， 第25欄第47行～第26欄第5行，第29欄第3行～第30欄 第43行，第31欄第32－37行，第1，2，5－8図 &　EP　1302944　A1 &　EP　1302945　A1 &　US　2002／157012　A1 &　US　2002／184537　A1	1－8

[x] C欄の続きにも文献が列挙されている。　　[ ] パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 13．08．2004	国際調査報告の発送日　31.8.2004
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 早川　卓哉　　5Q　9295 電話番号　03－3581－1101　内線　3590

様式PCT／ISA／210（第2ページ）（2004年1月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／００６９００

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ　２００２－６３０７５　Ａ（ソニー株式会社） ２００２．０２．２８，第３欄第２６－３２行，第５欄第５－１８行，第６欄第１－７行及，第１図（ファミリーなし）	１－８
Ｙ	ＪＰ　２００１－１４４４１　Ａ（松下電器産業株式会社） ２００１．０１．１９，第１１欄第１９－４７行，第１４欄第３４行～第１５欄第３８行，第５，６，９図 ＆　ＥＰ　１０５０８８７　Ａ１ ＆　ＥＰ　１３０４７０２　Ａ１	４，７
Ｙ	ＪＰ　１０－１３４０３　Ａ（日本電気株式会社） １９９８．０１．１６，第７欄第２１－４１行，第９欄第２３行～第１１欄第２１行，第１－５図（ファミリーなし）	４，７
Ｙ	ＪＰ　１０－１２３９５０　Ａ（富士ゼロックス株式会社） １９９８．０５．１５，第１４欄第３２行～第１７欄第１２行，第２３欄第１行～第２４欄第２１行，第１，３－５，１８，１９図 ＆　ＥＰ　８３７３８３　Ａ１ ＆　ＵＳ　６１６１１８３　Ａ	４，７
Ａ	ＪＰ　１１－２５０５１２　Ａ（ソニー　デーアーデーツェー　オーストリア　アクチェンゲゼルシャフト）１９９９．０９．１７，全文，第１－９図 ＆　ＥＰ　８９９７３３　Ａ１ ＆　ＵＳ　６５３５８５８　Ｂ	１－８
Ａ	ＪＰ　２００１－２２９０１９　Ａ（東芝イーエムアイ株式会社） ２００１．０８．２４，全文，第１－９図（ファミリーなし）	１－８